RHENISH
GIRLS' HIGH SCHOOL

RGHS ICT ACCEPTABLE USE POLICY

The school's information technology resources, including email and Internet access, are provided for educational purposes. Rhenish Girls' High School believes that learners and teachers must have access to technology and services if they act in a responsible, efficient, courteous and legal manner. Internet access and selected content and services hosted there, offer a multitude of powerful and effective globally based educational resources and tools.

1. Each learner will be given a user name and password to the RGHS network
2. Each learner will be given a Rhenish email address and password
3. Each learner will be given a Google Class user name and email address, located in the cloud, where educational lessons, assessments and content are hosted
4. The school keeps its grade related data in a number of WCED Applications offsite and in D6 Principal, and uses D6 Communicator to share information with parents. This includes personal data, which is captured and stored for up to 5 years from when it was created.
5. Each learner is granted Internet access for study, research and educational purposes, and in order to use selected educational applications and tools.

The goal in providing these services is to enhance the educational development of our learners. Each learner and teacher is responsible for their use of technology, and adherence to the following policy is necessary for continued access to the school's technological resources:

I _____ (name) realise that the use of technology is a privilege and not a right. I accept the following:

Responsibility to myself
I will

- Act safely by not sharing personal information in any of my projects. I will not give out my family name, email address, home address, school name, city, country or other information that could help someone locate or contact me in person.
- Notify an adult immediately if I inadvertently encounter any inappropriate materials.
- Be aware of the opportunities and risks posed by new and emerging technologies and I will assess the personal risks of using any particular technology, and I will also behave safely and responsibly to limit those risks.
- Take responsibility for the care and safety of my own device. My device will be clearly labelled.
- Respect and protect the privacy of others.
- Use only assigned accounts.
- Respect and protect the integrity, availability, and security of all electronic resources.
- Observe all network security practices, as posted.
- Report security risks or violations to a teacher or network administrator.
- Conserve, protect, and share these resources with other learners and Internet users.
- Respect and protect the intellectual property of others.
- Respect and practice the principles of community.
- Communicate only in ways that are kind and respectful.

- Report threatening or discomforting materials to a teacher.

I may, if in accord with the policy above

- Design and post web pages and other material from school resources.
- Use direct communications such as IRC, online chat, or instant messaging with a teacher's permission.
- Install or download software, if also in conformity with laws and licenses, and under the supervision of a teacher.
- Use the resources for any educational purpose.

I will not

- Post identifying photos or videos of myself or any other learners or staff members.
- Share my passwords with another person.
- View, use, or copy passwords, data, or networks to which I am not authorized.
- Distribute private information about others or myself.
- Destroy or damage data, networks, or other resources that do not belong to me, without clear permission of the owner. Not infringe copyright (not making illegal copies of music, games, or movies!).
- Plagiarise.
- Intentionally access, transmit, copy, or create material that violates the school's code of conduct (such as messages that are pornographic, threatening, rude, discriminatory, or meant to harass).
- Intentionally access, transmit, copy, or create material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works).
- Use the resources to further other acts that are criminal or violate the school's code of conduct.
- Send spam, chain letters, or other mass unsolicited mailings.
- Buy, sell, advertise, or otherwise conduct business, unless approved as a school project.

Technology protection measures (or "Internet filters") shall be used by the school to block access to inappropriate information. However, no filtering system is fool proof, and therefore, each learner must take responsibility for the sites and material that they access.

Anything reposted by a learner will be treated in the same manner as if they were the original author.

Responsibility to others
I may not

- use any form of electronic communication to harass, intimidate, or bully anyone. Bullying using digital means is still regarded as bullying and carries serious consequences according to the Acceptable Use Policy of the school. It must be noted that bullying of any kind is a social problem and is thus a whole school responsibility. Normal courtesy and good manners apply as much in the cyber world as the real world.
- use my device to harm others or their work.
- post photographic images or video recordings of a person at school or at any school-related activity without their explicit permission.

- post photographic images or video recordings of a person or persons at school or of any school-related activity that could harm either the person or the school's name.
- take photographs or video recordings of anybody who is not aware of it or when asked not to record it.
- post any information if it: violates the privacy of others, jeopardizes the health and safety of others or is obscene or libelous.
- trespass in another's folders, work, or files or make use of their passwords.

I will treat blog and wiki spaces as I would a classroom space, and I will use appropriate and respectful language.

Responsibility to learning

- I will only use my device in class when I have permission from the teacher.
- My earphones will not be used during school hours (7:40 - 14:20), unless I have a teacher's explicit permission, and this includes break times.
- I will not use my mobile device to make phone calls during school hours or to communicate with anybody using any form of instant messaging.
- I agree that while at school the purpose of my device is learning. Using it for other purposes will deplete the battery which will prevent me from using it for learning.
- My device will always be charged, and I will arrive at school with it fully charged.
- If there is a problem with my device I will take it to the school technician immediately, so as not to interrupt my learning.
- I will not use my device to attempt to cheat in any assessment.
- I respect plagiarism and copyright laws.

Responsibility to protect resources
I may not

- Damage, change, or tamper with the hardware, software, settings or the network in any way.
- Interfere with the operation of the network or attempt to bypass Rhenish Girls' High School firewall and Internet content filters.
- Waste limited resources such as disk, server space or bandwidth.
- Connect to the internet via any connection (3G) except the school's WiFi network, during school hours. Any other internet connection, such as 3G, must be switched off if possible and the device priority pointed to the school's wireless network.
- Make excessive use of data on the school's network
- Use my school account to sign up for apps/websites unless instructed to do so by a teacher.

I will ensure that

- All unused apps on my device are closed during school hours, to prevent them from using unnecessary bandwidth and depleting my battery.
- I have virus protection software on my device, to prevent viruses from entering the school's network through my device.

Consequences for Violation

Violations of these rules may result in disciplinary action, including the loss of a learner's privileges to use the school's information technology resources.

Supervision and Monitoring
School and network administrators and their authorized employees monitor the use of information technology resources to help ensure that uses are secure and in conformity with this policy. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any learner or other person, or to protect people and property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement.

Each learner will be issued with a Google account for the duration of their time at Rhenish Girls' High School. This account will be terminated once the learner leaves Rhenish Girls' High School. It is the learner's own responsibility to transfer all data to a personal account before their school account is deleted.

The School Principal retains the right to be the final arbitrator of what is and is not appropriate content. Consequences for breach of this policy will be determined by the Principal and may include banning an individual from bringing their ICT device to school.

Lost or stolen devices
Each user is responsible for their own device and must use it responsibly and appropriately. Rhenish Girls' High School takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices. While school employees will advise learners on how to secure their devices, final responsibility for securing their device remains that of the user.

The school does not insure individuals private devices – each individual is responsible for the insurance and replacement of their device should it become lost, broken or stolen.

Acceptance
I am prepared to be held accountable for my actions and will accept the loss of privileges, or other appropriate consequences if these rules are violated.

Name of learner/user: _____

Signature of learner/user: _____ Date_____

Name of parent/guardian:_____

Signature of parent/guardian: _____ Date_____

NOTE: Parents please discuss these rules with your child to ensure they understand them. These rules also provide a good framework for your child's use of computers at home, at libraries, or anywhere.

Glossary and Definitions

1. Asynchronistic or Asynchronous: occurs at different times e.g. e-mail conversations.
2. Blogs: Weblogs (blogs) are online journals created by individuals or groups and stored on the Internet. They are usually text-based, but also include other media such as images, video and sound content. Blogs are an ideal space to write about personal ideas and opinions.
3. Browsers: tools to access the World Wide Web
4. Cloud computing: term used to describe delivering hosted services such as infrastructure, platform and software services to other devices on demand. It lessens the workload on the local machine (the computer that the user is using).
5. Communities of Practice (CoPs): a group of people who have a common interest or profession and who communicate and share information.
6. Creative Commons licences: a licensing system for creative content such as video, audio or text, which specifies to what extent other people may share content, modify it, or give it away for free, and to what extent they are obliged to acknowledge or credit the original authors.
7. Cyberbullying: Harassing, humiliating or threatening someone in cyberspace, by sending them nasty e-mails, posting malicious information, fake profiles or embarrassing photographs or comments on
8. social networking sites.
9. Cybercrime: computer crime or cybercrime is a form of crime where the Internet or computers are used as a medium to commit crime.
10. Cyberspace: The same as "Internet": the global network of interconnected computers and communication systems.
11. Cybersecurity: computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users.
12. Cyberstalking: individuals who keep track of other users' activities and information for no legitimate reason.
13. Dark Web: is World Wide Web content that exists on dark nets,networks which overlay the public Internet and require specific software, configurations or authorization to access and are often used for illegal or criminal activity. The Dark Web forms part of the Deep Web, the part of the Web not indexed by search engines. Wikipedia [Accessed August 2015]
14. Digital image: an image created by digital technology such as a digital camera, or imaging editing software.
15. Digital Literacy: the ability to find, discern, select and use online information appropriately.
16. Digital footprint: the collection of data, which includes images, videos and text, posted by an individual online.
17. e-Education: consists of e-Learning, e-Teaching, e-Awareness and all the administrative responsibilities connected to these actions.
18. e-Learning: a broad term that generally refers to any kind of learning that is done with a computer and Internet connection or other media like a CD-ROM. It is widely used by individuals, educational institutions and businesses. e-Learning includes m-Learning.
19. e-Mail: electronic mail, most commonly abbreviated e-mail and e-mail, is a method of exchanging digital messages.
20. Filtering: a process to deny access to certain websites or resources as defined in the filter.
21. Firewall: part of a computer system or network that is designed to block unauthorised access while permitting authorised communications.
22. Flaming: hostile and insulting interaction between Internet users.
23. Internet: a worldwide network that connects smaller networks together.
24. Information literacy: the ability to recognise the need for information; to find, organise and evaluate such information for effective decision making or problem-solving, to generate new knowledge and to apply these skills for effective life-long learning.
25. Information skills: the skills which underpin a learner's ability to define the purpose of an information task, locate resources of data, select, interpret and use information to complete a task.
26. IT (Information Technology): defined as the "study, designs, expansion, execution, preservation or supervision of computer based information systems, specifically on computer hardware and software functions."
27. ICTs (Information and Communication Technologies): defined as forms of technologies that are used to create, store, share or transmit, exchange information; radio, television, video, DVD, telephone (both fixed line and mobile phones), satellite systems, computer and network hardware and
28. software; as well as the equipment and services associated with these technologies, such as videoconferencing and electronic mail (UNESCO 2002).
29. Inter-operability: the degree to which different types of software and hardware can interact effectively with each other.
30. Malware: a malicious or intentionally or unintentionally damaging software programme.
31. Media: the means whereby the messages and images that we consume and create are transmitted. These include television, movies, video games, books, magazines, the Internet, cell-phones, advertising billboards, and more.
32. m-Learning: a broad term that generally refers to any kind of learning that is done with a cell-phone, supplied directly on the cell-phone, as an application, game or similar content – or accessed via the Internet.

33. Multimedia: media that combines two or more media of communication (text, graphics and sound etc.)
34. Netiquette: Netiquette is a set of social conventions that facilitate interaction over networks, such as mailing lists to blogs and forums. These conventions include actions not to be used online, such as flaming people (see above), cross-posting (posting adverts on multiple platforms), or trolling (provoking people).
35. Phishing scams: is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.
36. Plagiarism: "the wrongful appropriation, close imitation, or purloining and publication, of another author's language, thoughts, ideas, or expressions, and the representation of them as one's own original work". Wikipedia [Accessed August 2010].
37. Social Media: Interactive media or websites which permit interaction between users, to promote user-generated content or communications. Examples include blogs, Facebook, Twitter, and similar. Social Networking: online platforms that provide means of personal communications between
38. participants such as FaceBook, LinkedIn, Twitter, WhatsApp and many others.
39. Spam: is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately.
40. Spoofing: Spoofing, or decoying, is the practice of inundating online networks with bogus or incomplete files of the same name in an effort to frustrate traders and reduce unlawful downloading. It can also refer to any falsification, e.g. of a domain name, so as to redirect traffic to another
41. location.
42. Synchronistic or Synchronous: things which occur at the same time e.g. online chat.
43. Trolling: To provoke people online by deliberately making inappropriate, false, or unprofessional statements, so as to elicit a negative reaction.
44. URL (Uniform Resource Locator): address that identifies a specific website e.g. http://www.education.gov.za.
45. Viral branding: refers to marketing techniques that use pre-existing social networks to produce increases in brand awareness or to achieve other marketing objectives (such as product sales) through self-replicating (viral) processes.
46. White-list: An approved list; often used with regard to Internet content filtering, a whitelist only includes addresses (such as URLs or e-mail) that have been specifically vetted in advance. Whitelists specify which protocols, sites or persons are allowed to communicate, unlike blacklists which specify which protocols, sites or persons may NOT communicate.

Legislation

Act No. 11 of 1967 Performers' Protection Act
Act No. 42 of 1993 Animal Matters Amendment Act
Act No. 108 of 1996 Constitution of the Republic of South Africa
Act No. 65 of 1996 Films and Publications Act
Act No. 84 of 1996 South African Schools Act
Act No.13 of 2000 Independent Communications Authority of South Africa Act
Act No. 70 of 2002 Regulation of Interception of Communications and Provision of Communication-Related Information Act
Act No. 36 of 2005 Electronic Communications and Transactions Act
Act No. 38 of 2005 Children's Act
Act No. 31 of 2007 Education Laws Amendment Act
Act No. 32 of 2007 Criminal Law (Sexual Offences and Related Matters) Amendment Act
2008 A Bill of Responsibilities for the Youth of South Africa
B9 – 2009 Protection of Personal Information Bill

Policies

2010 Cyber Security Draft Policy: Department of Communications
2015 School Safety Policy: Department of Basic Education